UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/008,053	11/09/2001	Matthew Hur	50325-0590	2815

29989   7590   04/29/2005

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER
SHIFERAW, ELENI A

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 04/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	10/008,053	HUR, MATTHEW
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>*09 November 2001*</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>*09 November 2001*</u> is/are: a)☐ accepted or b)☒ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date <u>*11/26/2001*</u>.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

1.   Claims 1-32 are presented for examination.

Drawings

2.   The drawings, Figure 1-2, 3B, 4A-4B, 5A-5B, 6, and 7, are objected to because the office

no longer accepts hand written drawings.   Corrected drawing sheets in compliance with 37 CFR

1.121(d) are required in reply to the Office action to avoid abandonment of the application.

3.   Figures 1 and 2 should be designated by a legend such as --Prior Art-- because only that

which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37

CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application.

The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37

CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not

accepted by the examiner, the applicant will be notified and informed of any required corrective

action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

5.   Claims 1-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sprunk et al.

(Sprunk, Pub. No.: US 2005/0027985 A1) in view of Ganesan (Patent Number: 5,737,419).

As per claim 1 Sprunk teaches a method of registering a non-configured network device in a

telecommunications network, the method comprising the computer-implemented steps of:

        receiving a message from a first non-configured network device that requests network

services (Sprunk Fig. 3 No. 310, page 3 par. 0043 lines 6-10, and page 5 par. 5 lines 1-3);

        authenticating the first device based on a longer-lived symmetric key received from the

first device (Sprunk page 2 par. 0033);

        generating and providing a shorter-lived symmetric key to the first device based on

authenticating the longer-lived symmetric key (Sprunk Fig. 3 No. 320; key validity period);

        receiving a request from a second device to obtain a session key for secure

communications between the second device and the first device (Sprunk page 1 lines 12-20, and

page 3 par. 0043);

        generating and providing a symmetric session key to the second device for use in

subsequent secure peer-to-peer communications between the first device and the second device

without communication of either the first device or second device to a key management service

or authoritative authentication service (Sprunk page 3 par. 0042); and

        registering the first device in the network (Sprunk page 4 par. 0055).

        Sprunk does not explicitly teach the shorter-lived symmetric key.

        However Ganesan teaches the shorter-lived symmetric key (Ganesan col. 5 lines 2-7).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Ganesan within the system of Sprunk because the damage an attacker can cause by learning the short-lived key is significantly less than the damage which might be caused by compromise of long term key. (Ganesan col. 5 lines 2-7).

As per claims 8, 18, and 30-32, Sprunk teaches a method/medium/apparatus for distributing cryptographic keys in a data network, comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom (Sprunk page 1 par. 0012);

a processor (Sprunk Fig. 2A No. 222);

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

providing a registration service identifier that identifies an administrative entity to a first device and providing a unique identifier of the first device to the administrative entity (Sprunk page 5 par. 0067);

associating a device private key in a secure data repository that is accessible by the administrative entity (Sprunk page 4 par. 0055);

establishing a longer-lived symmetric key for the first device (Sprunk Fig. 3 No. 320, and page 5 par. 0068; key validity period);

authenticating the first device based on receiving the longer-lived symmetric key from the first device (Sprunk page 2 par. 0033, and page 5 par. 0068);

receiving a request from a second device to obtain a session key for secure

communications among the second device and the first device (Sprunk page 1 lines 12-20, and

page 3 par. 0043); and

generating and providing a symmetric session key to the second device for use

in subsequent secure peer-to-peer communications between the first device and the second

device without communication of either the first device or second device to a key management

service or authoritative authentication (Sprunk page 3 par. 0042).

Sprunk does not explicitly teach the shorter-lived symmetric key.

However Ganesan teaches the shorter-lived symmetric key (Ganesan col. 5 lines 2-7).

Therefore it would have been obvious to one having ordinary skill in the art at the time of

the invention was made to employ the teachings of Ganesan within the system of Sprunk because

the damage an attacker can cause by learning the short-lived key is significantly less than the

damage which might be caused by compromise of long term key. (Ganesan col. 5 lines 2-7).

As per claim 2, Sprunk and Ganesan teach all the subject matter as described above. In addition,

Ganesan teaches a method, wherein the shorter-lived symmetric key is encapsulated in a ticket

that includes data identifying a specified lifetime of the shorter-lived symmetric key (Ganesan

col. 4 lines 56-col 5 lines 2-7). The rational for combining are the same as claim 1 above.

As per claim 3, Sprunk and Ganesan teach all the subject matter as described above. In addition,

the combination of Sprunk and Ganesan teach a method, further comprising the steps of

receiving, at the second device, a request from the first device to obtain a session key on behalf

of both the first device and second device, wherein the request includes the shorter-lived

symmetric key of the first device (Sprunk page 5 par. 0071, and Ganesan col. 5 lines 2-7).

As per claim 4, Sprunk and Ganesan teach all the subject matter as described above. In addition,

Sprunk teaches a method, wherein the subsequent secure communications comprise successive

symmetric encryption and decryption operations using the symmetric session key, and wherein

the first device and second device carry out the subsequent secure communications without

contact with a key management service or registration service (Sprunk page 2 par. 0031, page 1

par. 0011 lines 12-20).

As per claim 5, Sprunk and Ganesan teach all the subject matter as described above. In addition,

Sprunk teaches a method, further comprising the steps of:

receiving a request from a first device that wishes to communicate securely with a second

device to register with a trusted registration service (Sprunk Fig. 1 No. 310);

authenticating the first device (Sprunk page 2 par. 0033); and

in response to authenticating the first device, providing a longer-lived symmetric key to

the first device (Sprunk Fig. 3 No. 320; key validity period).

As per claim 6, Sprunk and Ganesan teach all the subject matter as described above. In addition,

Sprunk teaches a method, further comprising the steps:

authenticating the first device to a trusted registration service (Sprunk page 4 par. 0055);

and

in response to authenticating the first device to the trusted registration service, providing

the longer-lived symmetric key to the first device (Sprunk Fig. 3 No. 320; key validity period).

As per claim 7, Sprunk and Ganesan teach all the subject matter as described above. In addition,

Sprunk teaches a method, further comprising the steps of:

providing trusted information to the trusted registration service that certifies that the first

device as a known device within a security realm (Sprunk page 5 par. 0067, and fig. 3 No. 310);

and

providing information identifying the registration service to the first device for use in

obtaining the longer-lived symmetric key (Sprunk Fig. 3 No. 320).

As per claims 9 and 19, Sprunk and Ganesan teach all the subject matter as described above. In

addition, Sprunk teaches a method/medium/apparatus, teaches a method wherein the step of

associating a device private key with a data repository comprises the steps of generating a public

key pair comprising a device public key and a device private key and storing the device private

key in a database or directory that is accessible to the administrative entity (Sprunk page 4 par.

0055).

As per claims 10 and 20, Sprunk and Ganesan teach all the subject matter as described above. In

addition, Sprunk teaches a method/medium/apparatus, wherein the step of associating a device

private key with a data repository comprises the steps of generating a public key pair comprising

a device public key and a device private key and registering the device private key with a

certification authority that is accessible to the administrative entity (Sprunk page 4 par. 0055).

As per claims 11 and 21, Sprunk and Ganesan teach all the subject matter as described above. In

addition, Sprunk teaches a method/medium/apparatus, wherein the step of establishing a longer-

lived symmetric key for the first device comprises the steps of:

generating information that provides assurance to a registration service that the first

device is a certified device (Sprunk page 5 par. 0068 and 0071); and

authenticating the first device to the registration service (Sprunk page 5 par. 0068 and

0071).

As per claims 12 and 22, Sprunk and Ganesan teach all the subject matter as described above. In

addition, Sprunk teaches a method/medium/apparatus, wherein the step of establishing a longer-

lived symmetric key for the first device comprises the steps of:

generating information that provides assurance to a registration service that the first

device is a certified device (Sprunk page 5 par. 0068 and 0071); and

authenticating the first device to the registration service by sending a first message from

the first device to the registration service that is encrypted using the device public key (Sprunk

page 5 par. 0068 and 0071 and page 1 par. 0013).

As per claims 13 and 23, Sprunk and Ganesan teach all the subject matter as described above. In

addition, Sprunk teaches a method/medium/apparatus, wherein generating information that

provides assurance to a registration service that the first device is a certified device comprises the

steps of creating and storing an association of a unique identifier of the first device and the

device public key in a secure database that is accessible to the registration service, and providing

the unique identifier from the first device to the registration service (Sprunk page 4 par. 0055,

and page 5 par. 0068).

As per claims 14 and 24, Sprunk and Ganesan teach all the subject matter as described above. In

addition, Sprunk teaches a method/medium/apparatus, wherein establishing a longer-lived

symmetric key comprises the steps of:

      generating the longer-lived symmetric key (Sprunk Fig. 3 No. 320);

      encrypting the longer-lived symmetric key using the device public key (Sprunk Fig. 3

No. 320, and page 3 par. 0044);

      encapsulating the encrypted longer-lived symmetric key in a device registration

ticket (Sprunk page 3 par. 0044 lines 1-3); and

      sending the device registration ticket to the device (Sprunk page 5 par. 0071 and page 3

par. 0044-0045).

As per claims 15 and 25, Sprunk and Ganesan teach all the subject matter as described above. In

addition, Sprunk teaches a method/medium/apparatus, wherein encapsulating the encrypted key

comprises encapsulating the encrypted longer-lived symmetric key with policy information in

the device registration ticket, wherein the policy information defines a validity interval of the

encrypted longer-lived symmetric key (Sprunk Fig. 3 No. 320, and page 3 par. 0046).

As per claims 16 and 26, Sprunk and Ganesan teach all the subject matter as described above. In

addition, the combination of Sprunk and Ganesan teach a method/medium/apparatus, wherein

generating and providing a short-term symmetric key to the first device includes the steps of

encapsulating the short-term symmetric key in a short-term ticket granting ticket with associated

policy information (Sprunk page 4 par. 0055, and Ganesan col. 4 lines 56-col 5 lines 2-7). The

rational for combing are the same as claim 8 above.

As per claims 17 and 27, Sprunk and Ganesan teach all the subject matter as described above. In

addition, the combination of Sprunk and Ganesan teach a method/medium/apparatus, wherein

the step of receiving a request from a second device to obtain a session key for secure

communications among the second device and the first device comprises the steps of:

      receiving a first short-term ticket granting ticket that includes the short-term

symmetric key of the first device (Ganesan col. 23 lines 60-col. 24 lines 13, and col. 5 lines 2-7);

      receiving a second short-term ticket granting ticket that includes the short-term

symmetric key of the second device (Ganesan col. 23 lines 60-col. 24 lines 13, and col. 5 lines 2-

7);

      decrypting the first and second short-term ticket granting tickets based on respective first

and second shared secret keys (Sprunk page 4 par. 0055, and Ganesan col. 4 lines 56-col 5 lines

2-7);

authenticating the short-term symmetric keys of the first device and second device based

on the respective first and second shared secret keys (Sprunk page 4 par. 0055, and Ganesan col.

4 lines 56-col 5 lines 2-7); and

generating and providing a symmetric session key to the second device for use in

subsequent secure peer-to-peer communications between the first device and the second device

without communication of either the first device or second device to a key management service

or authoritative authentication service (Ganesan col. 8 lines 21-32, and Sprunk page 3 par. 0042).

The rational for combining are the same as claim 8 above.

6.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867.

The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the

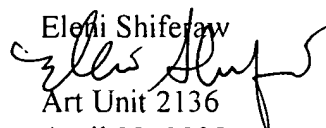organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw

Art Unit 2136

April 28, 2005

AYAZ SHEIKH

SUPERVISORY PATENT EXAMINER

TECHNOLOGY CENTER 2100